STIC EIC 2100 Search Request Form

17478

Today's Date: [redacted]-2005

What date would you like to use to limit the search?

Priority Date: 4/9/1999 Other:

Name Nadia Khoshnoodi

AU 2133 Examiner # 80432

Room # 2B65 Phone 2-3825

Serial # 09/719,193

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB

IEEE INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

(separat$ partition fragment$) ⇒ ① breaking apart an algorithm based on the data

near (cipher$; algorithm$)

(method; instruction$; [redacted])

(assign$ attribute delegate$ designate$) ⇒ ② assign a variable to each part of the algorithm

near (variable value register load)

"formal argument" function

③ apply non-linear transformation to each variable (representing algorithmic portions)

novelty:

algorithm is calculated based on the data which makes it less vulnerable to "Differential Key Differential Power Analysis" (DKDPA)

*already found US patent # 6,658,569 } Double-Patenting Ref.

STIC Searcher _____ Phone _____

Date picked up _____ Date Completed _____

sira Search and Information Resources Administration

Patent
FT

Set	Items	Description
S1	113273	ALGORITHM OR CIPHER? OR CYPHER?
S2	676886	DATA
S3	133366	(BASED()ON OR ACCORDING? OR CONTINGENT? OR EPENDING)(3N)S2
S4	1533	S1 (5N) S3
S5	347	S4 AND IC=H04L
S6	172	S5 AND AY=1978:1999
S7	77998	(BASED()ON OR ACCORDING? OR CONTINGENT? OR DEPENDENT? OR D-EPENDING)(3W)S2
S8	478	S1 (5N) S7
S9	103	S8 AND IC=H04L
S10	52	S9 AND AY=1978:1999
S11	52	IDPAT (sorted in duplicate/non-duplicate order)
S12	52	IDPAT (primary/non-duplicate records only)
S13	357	S1 (3N) S7
S14	83	S13 AND IC=H04L
S15	44	S14 AND AY=1978:1999
S16	44	IDPAT (sorted in duplicate/non-duplicate order)
S17	44	IDPAT (primary/non-duplicate records only)

File 348:EUROPEAN PATENTS 1978-2005/Dec W02
(c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20051215,UT=20051208
(c) 2005 WIPO/Univentio

6/5,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01262474
Data-aided and phase-independent adaptive equalization for data transmission systems
Datenunterstutzte und phasenunabhangige adaptive Entzerrung fur Daten-Ubertragungssysteme
Egalisation adaptative assistee par des donnees et independante de la phase pour des systemes de transmission de donnees

PATENT ASSIGNEE:
ALCATEL, (201871), 54, rue la Boetie, 75008 Paris, (FR), (Applicant designated States: all)
INVENTOR:
Frigerio, Marco, Via Don Sturzo, 12, 20059 Vimercate (Milano), (IT)
Spalvieri, Arnaldo, Via Ozieri, 4, 20100 Milano, (IT)
Valtolina, Roberto, Via Fratelli Bandiera, 6/A, 20056 Trezzo sull'Adda, (IT)
LEGAL REPRESENTATIVE:
Lamoureux, Bernard et al (83293), Compagnie Financiere Alcatel Departement de Propriete Industrielle, 5, rue Noel Pons, 92734 Nanterre Cedex, (FR)
PATENT (CC, No, Kind, Date): EP 1089457 A2 010404 (Basic)
EP 1089457 A3 040107
APPLICATION (CC, No, Date): EP 2000402588 000919;
PRIORITY (CC, No, Date): IT 99MI2009 990928
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04B-007/005; **H04L-025/03**

ABSTRACT EP 1089457 A2
A method and an equalizer is described for the adaptive equalization in a real- or complex- data transmission system, characterized by operating independently of the phase of the signal at the input of the equalizer but dependently of decided data. The equalizer comprises a FIR filter whose coefficients vary with time according to a determined cost function (J) given by where E((center dot)) indicates the averaging operation in relation to the symbols. In the event of combination of two or more signals in space diversity, the method allows for the coherent demodulation downstream of the equalizers.
ABSTRACT WORD COUNT: 97
NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	010404	A2	Published application without search report
Change:	030319	A2	Legal representative(s) changed 20030130
Change:	030402	A2	Legal representative(s) changed 20030210
Change:	040102	A2	International Patent Classification changed: 20031111
Search Report:	040107	A3	Separate publication of the search report
Withdrawal:	050420	A2	Date application deemed withdrawn: 20040708

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200114	679
SPEC A	(English)	200114	2502
Total word count - document A			3181
Total word count - document B			0
Total word count - documents A + B			3181

...INTERNATIONAL PATENT CLASS: **H04L-025/03**

...SPECIFICATION the CMA algorithms: thus, an algorithm has achieved which is a phase independent decision directed **algorithm** (PIDDA) **based on data** but independent of the phase, having the following cost function: where E((center dot)) denotes...

12/5,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01206035
System and method for network monitoring
Verfahren und Vorrichtung zur Netzwerkuberwachung
Methode et appareil pour la monitorisation de reseaux

PATENT ASSIGNEE:
Hewlett-Packard Company, A Delaware Corporation, (3016020), 3000 Hanover Street, Palo Alto, CA 94304, (US), (Applicant designated States: all)
INVENTOR:
Dowling, Brian M., 2440 Loch Way, El Eldorado Hills, California 95762, (US)
L'Ecuyer, Brian P., 9020 Poplar Hollow Lane, Elk Grove, California 95624, (US)
LEGAL REPRESENTATIVE:
Powell, Stephen David et al (52311), WILLIAMS, POWELL & ASSOCIATES 4 St Paul's Churchyard, London EC4M 8AY, (GB)
PATENT (CC, No, Kind, Date): EP 1049292 A2 001102 (Basic)
EP 1049292 A3 020605
APPLICATION (CC, No, Date): EP 2000303441 000425;
PRIORITY (CC, No, Date): US 303724 990430
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-012/26** ; **H04L-029/06**

ABSTRACT EP 1049292 A2
An algorithmic snoop unit (28) snoops interleaved transactions over a shared bus (42) as data is transmitted via transactions between clients (34, 36, 38) coupled to the shared bus, and executes various algorithms upon data snooped from the transactions. The unit includes one or more algorithmic entries (46, 48, 50) along with an algorithmic engine (44). Each algorithmic entry includes a client ID register that identifies the client associated with a transaction, a starting address register and an ending address that define the address range upon which an algorithm will be executed, a read or write flag that identifies whether the transactions is a read or write operation, an encryption key register for holding an encryption key, a decryption key register for holding a decryption key, an algorithm ID register for identifying an algorithm to be executed, a status/control register which holds various status and control, an accumulator for accumulating results from the execution of the algorithm, a temporary storage area, and one or more memory pointers that index a location in memory for results comprising a large amount of data. If a match is found, the algorithm identified by the algorithm ID register is executed upon the data carried by the transaction.
ABSTRACT WORD COUNT: 204
NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 001102 A2 Published application without search report
Assignee: 010502 A2 Transfer of rights to new applicant:
Hewlett-Packard Company, A Delaware Corporation (3016020) 3000 Hanover Street Palo Alto, CA 94304 US
Search Report: 020605 A3 Separate publication of the search report
Examination: 021120 A2 Date of request for examination: 20020923
Withdrawal: 030514 A2 Date of withdrawal of application: 20030319
LANGUAGE (Publication, Procedural, Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200044	482
SPEC A	(English)	200044	8283
Total word count - document A			8765

Total word count - document B 0
Total word count - documents A + B 8765

INTERNATIONAL PATENT CLASS: **H04L-012/26** ...
... **H04L-029/06**

...SPECIFICATION algorithmic entry specified by active algorithmic entries bus 94, algorithmic calculation unit 84 executes the **algorithm based on** the transaction **data** carried by data bus 98 and the operands stored in algorithmic entry control information registers...

...CLAIMS to determine if the algorithmic entry should be active for that transaction, and executes an **algorithm based on data** carried by the bus transaction for each active algorithmic entry.
2. The algorithmic snoop unit...

12/5,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01156735
SEMI-RELIABLE DATA TRANSPORT
HALB-ZUVERLASSIGER DATENTRANSPORT
TRANSPORT DE DONNEES SEMI-FIABLE
PATENT ASSIGNEE:
Enterasys Networks, Inc., (3943254), 50 Minuteman Road, Andover, MA 01810, (US), (Proprietor designated states: all)
INVENTOR:
KEMP, Bradford, H., 6 Lancelot Court 21, Salem, NH 03079, (US)
MCCANN, Benjamin, E., 16 Wilson Lane, Acton, MA 01720, (US)
LEGAL REPRESENTATIVE:
Power, Philippa Louise et al (95391), Frank B. Dehn & Co., 179 Queen Victoria Street, London EC4V 4EL, (GB)
PATENT (CC, No, Kind, Date): EP 1119955 A1 010801 (Basic)
EP 1119955 B1 040728
EP 1119955 B1 040728
WO 2000021262 000413
APPLICATION (CC, No, Date): EP 99951717 991001; WO 99US22919 991001
PRIORITY (CC, No, Date): US 167097 981005
DESIGNATED STATES (Pub A): AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; (Pub B): DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-029/06 ; H04L-001/18**
CITED PATENTS (EP B): US 5553083 A
CITED PATENTS (WO A): XP 2131820 ; XP 621327
CITED REFERENCES (EP B):
MARASLI R ET AL: "Partially reliable transport service" PROCEEDINGS. SECOND IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (CAT. NO.97TB100137), PROCEEDINGS SECOND IEEE SYMPOSIUM ON COMPUTER AND COMMUNICATIONS, ALEXANDRIA, EGYPT, 1-3 JULY 1997, pages 648-656, XP002131820 1997, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-7852-6
MARASLI R ET AL: "RETRANSMISSION-BASED PARTIALLY RELIABLE TRANSPORT SERVICE: AN ANALYTIC MODEL" PROCEEDINGS OF INFOCOM,US,LOS ALAMITOS, IEEE COMP. SOC. PRESS, vol. CONF. 15, 1996, pages 621-629, XP000621327 ISBN: 0-8186-7293-5;
CITED REFERENCES (WO A):
MARASLI R ET AL: "Partially reliable transport service" PROCEEDINGS. SECOND IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (CAT. NO.97TB100137), PROCEEDINGS SECOND IEEE SYMPOSIUM ON COMPUTER AND COMMUNICATIONS, ALEXANDRIA, EGYPT, 1-3 JULY 1997, pages 648-656, XP002131820 1997, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-7852-6
MARASLI R ET AL: "RETRANSMISSION-BASED PARTIALLY RELIABLE TRANSPORT SERVICE: AN ANALYTIC MODEL" PROCEEDINGS OF INFOCOM,US,LOS ALAMITOS, IEEE COMP. SOC. PRESS, vol. CONF. 15, 1996, pages 621-629, XP000621327 ISBN: 0-8186-7293-5;
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000607	A1	International application. (Art. 158(1))
Application:	000607	A1	International application entering European phase
Application:	010801	A1	Published application with search report
Examination:	010801	A1	Date of request for examination: 20010502
Examination:	021211	A1	Date of dispatch of the first examination report: 20021025
Assignee:	030618	A1	Transfer of rights to new applicant: Enterasys Networks, Inc. (3943254) 50 Minuteman Road Andover, MA 01810 US
Change:	030618	A1	Legal representative(s) changed 20030429

Grant: 040728 B1 Granted patent
Grant: 040728 B1 Granted patent
Oppn None: 050720 B1 No opposition filed: 20050429
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200431	747
CLAIMS B	(German)	200431	805
CLAIMS B	(French)	200431	865
SPEC B	(English)	200431	7772
Total word count - document A			0
Total word count - document B			10189
Total word count - documents A + B			10189

INTERNATIONAL PATENT CLASS: **H04L-029/06** ...

... **H04L-001/18**

...SPECIFICATION outbound data) prior to transmitting the third packet. The first software module implements a state- **dependent data** processing **algorithm** , such as a compression or an encryption algorithm, in which data processing of the outbound...

...CLAIMS processing raw outbound data for transmission from the source to the destination using a state- **dependent data** processing **algorithm** to produce outbound data wherein data processing of the raw outbound data depends on data...

12/5,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01140512
SELF-CORRECTIVE RANDOMIZER-ENCRYPTOR SYSTEM AND METHOD
SELBSTKORRIGIERENDES VERSCHLEIERUNGS-UND VERSCHLUSSELUNGSSYSTEM UND VERFAHREN
SYSTEME ET METHODE DE RANDOMISATION-CHIFFREMENT AUTOCORRECTEUR

PATENT ASSIGNEE:
Ferre Herrero, Angel Jose, (2882890), Avenida Constitucio 3 bis, 3., 43540 Sant Carles de la Rapita, (ES), (Proprietor designated states: all)
INVENTOR:
Ferre Herrero, Angel Jose, Avenida Constitucio 3 bis-3., 43540 Sant Carles de la Rapita, (ES)
LEGAL REPRESENTATIVE:
Ponti Sales, Adelaida et al (54403), Consell de Cent, 322, 08007 Barcelona, (ES)

PATENT (CC, No, Kind, Date): EP 1182777 A2 020227 (Basic)
EP 1182777 B1 031001
WO 2000008907 000224
APPLICATION (CC, No, Date): EP 99953987 991027; WO 99ES345 991027
PRIORITY (CC, No, Date): ES 991142 990518
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: **H04L-009/00**
CITED PATENTS (EP B): EP -0624013 A; EP -0676876 A; US 5220606 A; US 5608800 A

ABSTRACT EP 1182777 A2
Self-corrector randomising-encrypting system and method such that being supplied input data sequence (X) and control block (K) always generates randomised-encrypted data sequence, which is an at random number sequence.
Signature generating-assembly device (601) with data sequence (X) generates signed plaintext sequence (XF) supplied to randomising-encrypting device (102), where it is grouped with candidate control block (KC), which is generated by candidate control block generator (801) with control block (K), and generate suggested randomised-encrypted text sequence (AP) supplied to randomness verifier (603), which validates sequence randomness. If suggested randomised-encrypted text sequence (AP) is at random, it is supplied as randomised-encrypted text sequence (A); if it is not at random, the candidate control block generator (801) generates new candidate control block (KC) in order to randomise-encrypt the signed plaintext sequence (XF) again. The iteration is repeated until suggested randomised-encrypted text sequence (AP) is at random.
ABSTRACT WORD COUNT: 144

NOTE:
Figure number on first page: 8

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	020227 A2	Published application without search report
Application:	20000419 A1	International application. (Art. 158(1))
Lapse:	041006 B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20031001, CY 20031027, DK 20040101, FI 20031001, GR 20040101, NL 20031001, SE 20040101,
Lapse:	040901 B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20031001, CY 20031027, FI 20031001, GR 20040101, NL 20031001, SE 20040101,

Lapse:	040728 B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20031001, FI 20031001, SE 20040101,
Lapse:	040609 B1	Date of lapse of European Patent in a contracting state (Country, date): SE 20040101,
Grant:	031001 B1	Granted patent
Examination:	020227 A2	Date of request for examination: 20011114
Change:	030402 A2	International Patent Classification changed: 20030212
Change:	030402 A2	Title of invention (German) changed: 20030212
Change:	030402 A2	Title of invention (English) changed: 20030212
Assignee:	031126 B1	Transfer of rights to new proprietor: Etechnaf, S.L. (4561260) C. Senieta no. 3, Esc. B 2o 1o 43540 Sant Carles de la Rapita (Barcelona) ES
Change:	031126 B1	Inventor information changed: 20031008
Lapse:	040623 B1	Date of lapse of European Patent in a contracting state (Country, date): FI 20031001, SE 20040101,
Lapse:	040811 B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20031001, FI 20031001, GR 20040101, NL 20031001, SE 20040101,
Oppn None:	040922 B1	No opposition filed: 20040702
Application:	20000419 A1	International application entering European phase

LANGUAGE (Publication,Procedural,Application): English; English; Spanish
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200209	13404
CLAIMS B	(English)	200340	4441
CLAIMS B	(German)	200340	4336
CLAIMS B	(French)	200340	5954
SPEC A	(English)	200209	25777
SPEC B	(English)	200340	25517
Total word count - document A			39188
Total word count - document B			40248
Total word count - documents A + B			79436

INTERNATIONAL PATENT CLASS: **H04L-009/00**

...SPECIFICATION you can have to repeat this process successively. It is worth mentioning the existence of **ciphering** devices that operate **according** to the input **data** , which can be either the **encryption key or the plaintext message data. Some examples of...**

...SPECIFICATION you can have to repeat this process successively. It is worth mentioning the existence of **ciphering** devices that operate **according** to the input **data** , which can be either the encryption key or the plaintext message data. Some examples of...

17/5,K/14 (Item 14 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00661290
Design and managing method for communication networks
Entwurfs- und Verwaltungsverfahren fur Kommunikationsnetze
Procede de conception et de gestion pour reseau de communications
PATENT ASSIGNEE:
FUJITSU LIMITED, (211460), 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa 211, (JP), (Proprietor designated states: all)
INVENTOR:
Iwakawa, Akinori, c/o Fujitsu Limited, 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa 211, (JP)
Niu, Zhisheng, c/o Electronic Engineering Dept., Tsinghua University Qing Hua Yuan, Beijing, 100084, (CN)
Abe, Shunji, c/o Fujitsu Limited, 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa 211, (JP)
LEGAL REPRESENTATIVE:
Lehn, Werner, Dipl.-Ing. et al (7474), Hoffmann Eitle, Patent- und Rechtsanwalte, Arabellastrasse 4, 81925 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 635958 A2 950125 (Basic)
EP 635958 A3 000112
EP 635958 B1 050720
APPLICATION (CC, No, Date): EP 94111392 940721;
PRIORITY (CC, No, Date): JP 94165704 940719; JP 93180476 930721; JP 93320316 931220
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **H04L-012/24** ; **H04L-012/56** ; H04Q-003/00
CITED PATENTS (EP B): US 5119367 A; US 5153877 A
CITED REFERENCES (EP B):
HISAO UOSE ET AL: "DESIGN AND CONTROL ASPECTS OF ATM TRANSIT NETWORKS. \-TOWARDS THE FLEXIBLE NETWORK-" PROCEEDINGS OF THE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS),US,NEW YORK, IEEE, vol. -, page 361-372 XP000344708 ISBN: 0-7803-0588-4
GERSHT A ET AL: "REAL-TIME BANDWIDTH ALLOCATION AND PATH RESTORATIONS IN SONET-BASED SELF-HEALING MESH NETWORKS" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC),US,NEW YORK, IEEE, vol. -, page 250-255 XP000371102 ISBN: 0-7803-0950-2
ANEROUSSIS N G ET AL: "A MULTIPROCESSOR ARCHITECTURE FOR REAL-TIME EMULATION OF MANAGEMENT AND CONTROL OF BROADBAND NETWORKS" PROCEEDINGS OF THE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS),US,NEW YORK, IEEE, vol. -, page 346-360 XP000344707 ISBN: 0-7803-0588-4;

ABSTRACT EP 635958 A2
A designing and managing system for a communications network comprising a physical network and a logical network provides a designing system for flexibly corresponding to a traffic fluctuation through a simple procedure, and a managing system for quickly selecting an applicable communications path in response to a path connection request and a path capacity change request. The designing system comprises units (1 and 2) for respectively determining the topologies of the physical network and the logical network independently of traffic conditions, units (3 and 4) for setting the path capacities of the physical network and the logical network respectively based upon a long-term traffic demand and an actual request. The managing system comprises a unit for registering the limited number of detour path candidates, a unit for determining the existence of a detour path in response to a virtual path connection request, and a unit, provided in a start point node of a communications path, for determining the acceptability of a change in the capacity of a path based on a value of a space size of each link forming part of the communications path. (see image in original document)
ABSTRACT WORD COUNT: 192
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Examination:	010502 A2	Date of dispatch of the first examination report: 20010314
Change:	20000112 A2	International Patent Classification changed: 19991120
Grant:	050720 B1	Granted patent
Application:	950125 A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	20000112 A3	Separate publication of the search report
Examination:	20000412 A2	Date of request for examination: 20000215
Change:	950405 A2	Inventor (change)

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200529	3014
CLAIMS B	(German)	200529	2740
CLAIMS B	(French)	200529	3872
SPEC B	(English)	200529	17645
Total word count - document A			0
Total word count - document B			27271
Total word count - documents A + B			27271

INTERNATIONAL PATENT CLASS: **H04L-012/24** ...

... **H04L-012/56**

...SPECIFICATION the logical network independently of the traffic condition by executing a logical network topology design **algorithm** **according** to **data** on a number of nodes stored in the first data base (35); physical network capacity...

...CLAIMS the logical network independently of the traffic condition by executing a logical network topology design **algorithm** **according** to **data** on a number of nodes stored in the first data base (35); physical network capacity...

17/5,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00638686
Method of file signature and device for performing the method
Verfahren zur Dateiunterschrift und Einrichtung fur seine Durchfuhrung
Procede de signature d'un fichier informatique et dispositif pour la mise en oeuvre

PATENT ASSIGNEE:
BULL CP8, (753213), 68 route de Versailles, B.P. 45, 78430 Louveciennes, (FR), (Proprietor designated states: all)
INVENTOR:
Ugon, Michel, 6, rue des Cepages, F-78310 Maurepas, (FR)
LEGAL REPRESENTATIVE:
Corlu, Bernard et al (60535), CP8, Direction de la Propriete Intellectuelle 36-38, Rue de la Princesse, BP 45, 78431 Louveciennes Cedex, (FR)

PATENT (CC, No, Kind, Date): EP 619660 A1 941012 (Basic)
EP 619660 B1 020410
APPLICATION (CC, No, Date): EP 94400739 940405;
PRIORITY (CC, No, Date): FR 934073 930406
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: **H04L-009/32** ; G07F-007/10
CITED PATENTS (EP B): EP 77238 A; EP 281225 A
CITED REFERENCES (EP B):
IEEE INFOCOM '92 PROCEEDINGS, FLORENCE IT, IEEE NEW YORK US pages 2045 - 2054 Y. DESMEDT ET AL. 'Multi-receiver/multi-sender network security: efficient authenticated multicast/feedback'
NTT REVIEW, vol.5, no.1, Janvier 1993, TOKYO JP pages 75 - 81 T. OKAMOTO ET AL. 'On comparison of practical digital signature schemes';

ABSTRACT EP 619660 A1 (Translated)
The invention relates to a method of signing a main computer file (FP), of the type consisting in making circuits of an information processing device (1,3,4) calculate at least one signature (SG) of the file, taking into account at least one secret data item (S; Sd) specific to the signatory, but unknown to the latter, memorised in a secret memory area of a portable electronic object (4), with a memory and processing circuits, available to the signatory, and in linking the calculated signature to the main file.
It is characterised in that, upon the calculation of each signature, it further consists in taking account of at least a part of the main file, so that the signature is a function of the secret data item of the signatory and of each part of the file taken into account, and in creating a secondary file (FS) and in writing therein at least some information (IN) making it possible to identify each part of the main file having served for the calculation of this signature, and in linking the secondary file, on the one hand to the corresponding signature, and, on the other hand, to the signed file.
TRANSLATED ABSTRACT WORD COUNT: 199

ABSTRACT EP 619660 A1
L'invention concerne un procede de signature d'un fichier principal (FP) informatique, du genre consistant a faire calculer, par des circuits d'un dispositif (1,3,4) de traitement de l'information, au moins une signature (SG) du fichier, en prenant en compte au moins une donnee secrete (S; Sd) propre au signataire, mais inconnue de celui-ci, memorisee dans une zone de memoire secrete d'un objet portatif electronique (4), a memoire et circuits de traitement, a la disposition de ce signataire, et a lier la signature calculee au fichier principal.
Il est caracterise en ce que, lors du calcul de chaque signature, il consiste en outre a prendre en compte, au moins une partie du fichier principal, de sorte que la signature est fonction de la donnee secrete du

signataire et de chaque partie prise en compte du fichier, et a creer un fichier secondaire (FS) et y inscrire au moins des informations (IN) permettant d'identifier chaque partie du fichier principal ayant servi au calcul de cette signature, et a lier le fichier secondaire d'une part a la signature correspondante et d'autre part au fichier signe. (voir 1 image dans le document original)

ABSTRACT WORD COUNT: 190

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	010829	A1	Legal representative(s) changed 20010712
Application:	941012	A1	Published application (A1with Search Report ;A2without Search Report)
Lapse:	030507	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20020410, GR 20020410,
Lapse:	030305	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20020410,
Change:	020109	A1	Legal representative(s) changed 20011116
Grant:	020410	B1	Granted patent
Oppn None:	030402	B1	No opposition filed: 20030113
Examination:	941123	A1	Date of filing of request for examination: 940926
Examination:	970813	A1	Date of despatch of first examination report: 970630

LANGUAGE (Publication,Procedural,Application): French; French; French

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(French)	EPABF2	1568
CLAIMS B	(English)	200215	1238
CLAIMS B	(German)	200215	1210
CLAIMS B	(French)	200215	1273
SPEC A	(French)	EPABF2	6629
SPEC B	(French)	200215	6473
Total word count - document A			8198
Total word count - document B			10194
Total word count - documents A + B			18392

INTERNATIONAL PATENT CLASS: **H04L-009/32** ...

...CLAIMS S, Sd);

- recalculating the signature in the device by executing a **calculation with the signature algorithm , based on the secret data** item in the secret memory zone and on the identified chosen file portion, and taking...

...SG) by using a signature algorithm (Aa, Ao) and by executing a calculation with this **algorithm , based on** the secret **data** item of the portable object and on the file, a result of this calculation constituting...

17/5,K/32 (Item 32 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00557889 **Image available**
SEMI-RELIABLE DATA TRANSPORT
TRANSPORT DE DONNEES SEMI-FIABLE
Patent Applicant/Assignee:
INDUS RIVER NETWORKS INC,
KEMP Bradford H,
MCCANN Benjamin E,
Inventor(s):
KEMP Bradford H,
MCCANN Benjamin E,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200021262 A1 20000413 (WO 0021262)
Application: WO 99US22919 19991001 (PCT/WO US9922919)
Priority Application: US 98167097 19981005
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: **H04L-029/06**
International Patent Class: **H04L-001/18**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9169

English Abstract
A new type of communication protocol provides semi-reliable transport of data over a data channel, such as over the Internet. The new type of protocol limits the number of retransmissions of unsuccessfully delivered data and may eventually "give up" on successfully delivering particular data and go on sending subsequent data to the destination. When a reliable communication protocol, such as TCP/IP is tunneled between two computers over a virtual connection which uses the new type of semi-reliable protocol, overall error control of data passing between the two computers involves elements of error control implemented by both the semi-reliable protocol and the reliable protocol. This overall error control can provide higher throughput than provided by using either a completely reliable protocol (e.g., TCP) for the virtual connection, or a completely unreliable protocol (e.g., UDP) for the virtual connection. This advantage can be even more pronounced if the data stream is compressed or encrypted before being passed over the virtual connection using a technique which maintains state from one data packet to another.

French Abstract
Ce nouveau type de protocole de communication assure un transport de donnees semi-fiable sur un canal de donnees, sur l'Internet par exemple. Ce nouveau type de protocole limite le nombre de retransmissions de donnees non delivrees et peut finalement delaisser la delivrance menee a bonne fin de donnees particulieres et envoyer des donnees subsequentes vers leur destination. Lorsqu'un protocole fiable de communication, par exemple TCP/IP est soumis a un effet tunnel entre deux ordinateurs sur une connexion virtuelle utilisant ce nouveau type de protocole semi-fiable, le traitement d'erreur global passant entre les deux ordinateurs met en jeu des elements de traitement d'erreur

implementes tant par le protocole semi-fiable que par le protocole fiable. Ce traitement d'erreur global assure un debit de traitement superieur a celui obtenu au moyen d'un protocole totalement fiable (TCP, par exemple) pour la connexion virtuelle ou au moyen d'un protocole totalement depourvu de fiabilite (UDP, par exemple) pour la connexion virtuelle. Cet avantage est encore plus manifeste si le train de donnees est compresse ou chiffre avant de passer par la connexion virtuelle et ce, par utilisation d'une technique maintenant un etat d'un paquet de donnees a un autre.

Main International Patent Class: **H04L-029/06**
International Patent Class: **H04L-001/18**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... outbound data) prior to
transmitting the third packet.

The first software module implements a state **dependent data** processing **algorithm** , such as a compression or an encryption algorithm, in which data processing of the outbound...

Claim
... 6 The method of claim 1 further comprising processing raw outbound data using a state- **dependent data** processing **algorithm** to produce the outbound data wherein data processing of the raw outbound data 5 depends...

17/5,K/35 (Item 35 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00516884 **Image available**
SECURITY SYSTEM AND METHOD FOR BUSINESS TRANSACTIONS WITH CUSTOMERS
SYSTEME ET PROCEDE DE SECURITE DESTINES A DES TRANSACTIONS COMMERCIALES AVEC DES CLIENTS

Patent Applicant/Assignee:
FIRST UNION CORPORATION,
Inventor(s):
MORRISON William T Jr,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9948236 A2 19990923
Application: WO 99US4041 19990225 (PCT/WO US9904041)
Priority Application: US 9844503 19980319
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: **H04L**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10408

English Abstract
A security system and method by which customers may be readily identified prior to cashing of checks, other cash-out transactions, or other business transactions, wherein each customer is issued an individualized customer identification card having at least a personalized multidigit customer identification number encoded thereon and, optionally, also encoded with additional personal data identifying the customer. To cash a check or conduct another form of business transaction, whether at an attended customer service station or at an automated machine, the encoded data on the identification card is read and the customer is required to input the personalized identification number assigned to the card. The transaction is not approved unless the customer correctly inputs the assigned identification number. In contemplated embodiments, the encoded data along with data regarding the transaction requested by the customer, e.g., obtained by optical scanning of a check or other item presented by the customer, is transmitted to a central computer system for execution of an approval-disapproval analysis or algorithm.

French Abstract
L'invention concerne un systeme et un procede de securite permettant d'identifier facilement des clients avant l'encaissement de cheques, d'autres transactions de paiement ou d'autres transactions commerciales, chaque client etant dote d'une carte d'identification de client personnalisee codee avec au moins un numero d'identification personnel de client a plusieurs chiffres et eventuellement codee egalement avec des donnees personnelles supplementaires identifiant le client. Pour l'encaissement d'un cheque ou pour une autre forme de transaction commerciale, que ce soit a un guichet pour clients ou a une machine automatique, les donnees codees sur la carte d'identification sont lues et le client est prie d'entrer le numero d'identification personnel attribue a la carte. La transaction ne s'effectue pas tant que le client

n'entre pas correctement le numero d'identification attribue. Dans des modes de realisation prevus, les donnees codees et les donnees concernant la transaction demandee par le client, obtenues par exemple par balayage optique d'un cheque ou d'un autre produit presente par le client, sont transmises ensemble a un systeme informatique central qui execute une analyse ou un algorithme d'approbation-desapprobation.

Main International Patent Class: **H04L**
Fulltext Availability:
Claims

Claim
... for executing upon each cash-out
30
transaction requested by the customer an approval-disapproval **algorithm based on** the historical **data** on the customer.

28. A security method for use by a business for establishing customer ...determination of approval or disapproval of each cash-out transaction comprises executing an approval-disapproval **algorithm based on** the historical **data** on the customer

17/5,K/36 (Item 36 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00510338 **Image available**
METHODS AND APPARATUS FOR INTERNET BASED FINANCIAL TRANSACTIONS WITH EVIDENCE OF PAYMENT
PROCEDE ET DISPOSITIF POUR TRANSACTIONS FINANCIERES INTERNET AVEC TRACE DE PAIEMENT

Patent Applicant/Assignee:
SARANAC SOFTWARE INC,
Inventor(s):
LEWIS Richard,
DWYER Tara,
ABDELSADEK Mohammed,
HAN Donald,
ROGOFF Jonathon,
PARKS Louis,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9941690 A1 19990819
Application: WO 99US3099 19990212 (PCT/WO US9903099)
Priority Application: US 9823724 19980213
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: G06F-017/60
International Patent Class: **H04L-009/00**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22355

English Abstract
A system and method for conducting Internet-based financial transaction between a client (2n) and a server (4). The client has a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature. The server has a network including a transaction server (180), a transaction database (170), a server authentication module, and a receipt generation module. An Internet connection (30) is used between the client (2n) and the server network (4). The transaction execution system includes authentication, wherein the client authentication module and the server authentication modules communicate via the Internet connection (30) and are authenticated to each other. A transaction module is included wherein, in response to the client and server being authenticated, the client (2n) issues a transaction request to the server (4) and the transaction server (180), in response to a client transaction request, executes an electronic payment transaction at the server and records the transaction in the transaction database (170). The server receipt generation module, in response to an executed electronic payment, then generates a receipt and transmits the receipt to the client (2n).

French Abstract
L'invention concerne un systeme et un procede permettant les transactions financieres Internet entre un client (2n) et un serveur (4). Le client dispose d'un processeur, d'une imprimante, d'un module d'authentification de client, d'un module de demande de transaction et

d'une empreinte numerique propre. Le serveur dispose d'un reseau comprenant un serveur de transaction (180), une base de donnees de transactions (170), un module d'authentification de serveur et un module d'etablissement de recu. Une liaison Internet (30) est etablie entre le client (2n) et le reseau du serveur (4). Le systeme d'execution de transaction procede a l'authentification, moyennant quoi le module d'authentification du client et le module d'authentification du serveur communiquent entre eux sur ladite liaison (30) et s'identifient mutuellement. Le module de transaction fonctionne comme suit: apres l'authentification du client et du serveur, le client (2n) envoie une demande de transaction au serveur (4) et, en reponse a cette demande, le serveur de transaction (180) execute une transaction de paiement electronique a l'echelon du serveur, avec enregistrement dans la base de donnees (170). Suite a ladite execution, le module d'etablissement de recu du serveur etablit un recu qu'il transmet au client (2n).

International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... client private key, and a client identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the client public key, private key and identification...
...server private key, and a server identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the server public key, private key and identification...a client private key, a client identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the client public key, private key and identification...

...a server private key, a server identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the server public key, private key and identification...

Claim
... client private key, and a client identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the client public key, private key and identification...

...server private key, and a server identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the server public key, private key and identification...a client private key, a client identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the client public key, private key and identification...

...a server private key, a server identification password, a hash module for performing a hash **algorithm based on** an input **data** , a hash of at least one of the server public key, private key and identification...

17/5,K/38 (Item 38 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00447207 **Image available**
AN ADAPTIVE PRE-EQUALIZER FOR USE IN DATA COMMUNICATIONS EQUIPMENT
PRE-EGALISEUR ADAPTABLE POUR UTILISATION DANS UN EQUIPEMENT DE TRANSMISSION DE DONNEES

Patent Applicant/Assignee:
GLOBESPAN TECHNOLOGIES INC,
Inventor(s):
HERZBERG Hanan,
LANGBERG Ehud,
WANG Jin-Der,
WERNER Jean-Jacques,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9837671 A1 19980827
Application: WO 97US2758 19970225 (PCT/WO US9702758)
Priority Application: WO 97US2758 19970225
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
BR CA CN JP KR MX RU AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-025/03**
International Patent Class: **H04L-25:49** ; H04B-15:00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 5475

English Abstract
The problem of error propagation is addressed by using the communications channel (15) to adapt a pre-equalizer of a transmitter (10) to the changes in the response of the communications channel (15). In particular, the pre-equalizer adapts to changes in the communications channel (15) by processing an error signal that is communicated over a reverse channel (16) by a corresponding receiver (20).

French Abstract
L'invention vise a resoudre le probleme de la propagation d'erreurs, au moyen d'une voie de communication (15) servant a adapter un pre-egaliseur d'un emetteur (10) aux modifications de reponse de la voie de communication (15). En particulier, le pre-egaliseur s'adapte aux modifications dans la voie de communication (15), par traitement d'un signal d'erreur qui est transmis sur une voie de retour (16) par un recepteur correspondant (20).
Main International Patent Class: **H04L-025/03**
International Patent Class: **H04L-25:49** ...
Fulltext Availability:
Detailed Description

Detailed Description
... data available in receiver 20 for the K samples (whereas the adaptation of the sign **algorithm** is **based on** one sample per **data** block of length K), and 0 avoiding the need for synchronization between j(n) and...

17/5,K/43 (Item 43 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00390706 **Image available**
COMMUNICATION METHOD USING COMMON CRYPTOGRAPHIC KEY
METHODE DE COMMUNICATION UTILISANT UNE CLE CRYPTOGRAPHIQUE COMMUNE

Patent Applicant/Assignee:
CARD CALL SERVICE CO LTD,
Inventor(s):
BABA Yoshimi,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9731449 A1 19970828
Application: WO 97JP433 19970219 (PCT/WO JP9700433)
Priority Application: JP 9670832 19960221; JP 9670835 19960221; JP 96210376 19960708
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU BG BR CA CN CU CZ HU IL KR LT MX NO NZ PL RO RU SG SK TR UA VN
Main International Patent Class: **H04L-009/08**
Publication Language: Japanese

English Abstract
A communication method using a common cryptographic key by which security against various kinds of attacks can be improved while the preparation of a common cryptographic key prepared at the time of performing communication or a cryptographic communication system on a network is simplified. At a center, a personal key peculiar to each entity is prepared by applying Fourier transformation with weight function and center matrix to the identifier of each entity (procedures 2-1 and 2-2) and performing randomized transformation based on one-time random number data prepared by artificial processing of the entities (procedures 2-3 to 2-5) and, at the same time, an identifier converting **algorithm** is prepared **based on** the random number **data** and Fourier transformation with weight function (procedure 2-6) and distributes the algorithm and personal keys to the entities. Each entity prepares a common key used for performing cryptographic communication with a partner by applying the identifier converting algorithm and personal key to the identifier of the partner.

French Abstract
Methode de communication utilisant une cle cryptographique commune, ce qui permet d'**ameliorer la securite contre des atteintes** diverses tout en simplifiant la preparation de cette **cle cryptographique commune** au moment de la communication ou le systeme de communication cryptographique sur un reseau. Au niveau d'un centre, une cle personnelle specifique a chaque entite est elaboree en appliquant une transformee de Fourier avec fonction de ponderation et matrice centrale a l'identifieur de chaque entite (procedure 2-1 et 2-2) et en accomplissant une transformation aleatoire sur la base de donnees numeriques aleatoires a usage unique etablies par traitement artificiel des entites (procedure 2-3 et 2-5) tandis que, simultanement, un algorithme convertisseur d'identifieur est etabli sur la base des donnees numeriques aleatoires et de la transformee de Fourier avec fonction de ponderation (procedure 2-6) et que l'algorithme et les cles personnelles sont distribues aux entites. Chaque entite etablit une cle commune utilisee pour la communication cryptographique avec un partenaire en appliquant l'algorithme convertisseur d'identifieur et la cle personnelle a l'identifieur du partenaire.

Main International Patent Class: **H04L-009/08**

English Abstract

...entities (procedures 2-3 to 2-5) and, at the same time, an identifier converting **algorithm** is prepared **based on** the random number **data** and Fourier transformation with weight function (procedure 2-6) and distributes the algorithm and personal...

Patent Bib

```
Set     Items   Description
S1       7769   CIPHER? OR CYPHER?
S2      37805   ALGORITHM? ?
S3    1725533   DATA
S4     126202   (BASED()ON OR ACCORDING? OR CONTINGEN
           EPENDING)(3W)S3
S5        232   (S1 OR S2) (5N) S4
S6         89   S5 AND IC=G06F
S7         25   S6 AND AY=1963:1999
S8         25   IDPAT (sorted in duplicate/non-duplicate order)
S9         25   IDPAT (primary/non-duplicate records only)
S10   4964973   VALUE? ? OR NUMBER? ? OR INFORMATION OR TERM? ? OR TEXT OR
           WORD? ?
S11    255635   (BASED()ON OR ACCORDING? OR CONTINGENT? OR DEPENDENT? OR D-
           EPENDING)(3W)S10
S12       388   (S1 OR S2) (5N) S11
S13       125   S12 AND IC=H04L
S14        38   S13 AND AY=1963:1999
S15        38   S14 NOT S9
S16        38   IDPAT (sorted in duplicate/non-duplicate order)
S17        38   IDPAT (primary/non-duplicate records only)
S18        65   S5 AND IC=H04L
S19        18   S18 AND AY=1963:1999

S20        13   S19 NOT (S9 OR S17)
S21        13   IDPAT (sorted in duplicate/non-duplicate order)
S22        13   IDPAT (primary/non-duplicate records only)
S23        34   S18 AND PY=1976:1999
S24        22   S23 NOT (S9 OR S17 OR S22)
S25        22   IDPAT (sorted in duplicate/non-duplicate order)
S26        22   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2005/Jul(Updated 051102)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200581
        (c) 2005  Thomson Derwent
```

9/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014685920 **Image available**
WPI Acc No: 2002-506624/200254
XRPX Acc No: N02-400800
Computer file requests latency reduction in Internet, involves accessing file whose access probability exceeds or equals server's prefetch threshold value, if there is no current copy of file available on computer
Patent Assignee: UNIV CALIFORNIA (REGC)
Inventor: JIANG Z; KLEINROCK L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6385641	B1	20020507	US 9892108	A	19980605	200254	B

Priority Applications (No Type Date): US 9892108 A 19980605
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6385641	B1		30	G06F-015/16	

Abstract (Basic): US 6385641 B1
NOVELTY - An access probability for each computer file is computed using an application specific **algorithm , based on data** regarding file access at requested local computer. A prefetch threshold is calculated using a specific algorithm, based on current network conditions of each server. Each file whose access probability exceeds or equals server's prefetch threshold is accessed, if there is no current copy of file in the computer.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for computer files request latency reduction apparatus.
USE - For reducing latency of request for files in computer in network such as Internet.
ADVANTAGE - The files to be prefetched are determined by the access probability, to minimize the average cost of requesting a file. Hence the operation efficiency is improved.
DESCRIPTION OF DRAWING(S) - The figure shows the simple flow diagram of computer files request latency reduction process.
pp; 30 DwgNo 14/16
Title Terms: COMPUTER; FILE; REQUEST; LATENT; REDUCE; ACCESS; FILE; ACCESS; PROBABILITY; EQUAL; SERVE; THRESHOLD; VALUE; NO; CURRENT; COPY; FILE; AVAILABLE; COMPUTER
Derwent Class: T01
International Patent Class (Main): **G06F-015/16**
International Patent Class (Additional): **G06F-015/177**
File Segment: EPI

9/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014018856 **Image available**
WPI Acc No: 2001-503070/200156
XRPX Acc No: N01-373096

Electronic security key for electronic coin acceptor, has encryption algorithm that generates encrypted password data which is transmitted to electronic coil acceptor, to enable coin programming

Patent Assignee: IDX INC (IDXI-N)
Inventor: JUDS S
Number of Countries: 004 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CA 2323844	A1	20010515	CA 2323844	A	20001019	200156	B
AU 200066536	A	20010712	AU 200066536	A	20001016	200156	
GB 2357620	A	20010627	GB 200024934	A	20001011	200156	
AU 753887	B	20021031	AU 200066536	A	20001016	200282	
US 6564997	B1	20030520	US 99439995	A	19991115	200336	
GB 2357620	B	20031203	GB 200024934	A	20001011	200403	
CA 2323844	C	20051018	CA 2323844	A	20001019	200570	

Priority Applications (No Type Date): US 99439995 A 19991115
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CA 2323844	A1	E	49	H04L-009/32	
AU 200066536	A			G06F-007/02	
GB 2357620	A			G07D-005/00	
AU 753887	B			G07D-005/00	Previous Publ. patent AU 200066536
US 6564997	B1			G06K-005/00	
GB 2357620	B			G07D-005/00	
CA 2323844	C	E		H04L-009/32	

Abstract (Basic): CA 2323844 A1

NOVELTY - The electronic security key circuit includes microcontroller which transmits request message to the coin acceptor to transmit the identification number data and random number data generated by coin acceptor. **Based on** transmitted requested **data**, an encryption **algorithm** generates a password data and transmits to electronic coin acceptor, to effect an enabled state of coin acceptor for coin programming.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for tilt illuminator.

USE - For electronic coin acceptor in coin operated game devices such as slot machine and video poker machine.

ADVANTAGE - By transmitting an encrypted password data to electronic coin acceptor to effect enable state for coin programming, the tracking of individuals making changes in coin acceptor program is enabled and hence the individuals responsible for current coin acceptor programs is identified easily. Since encrypted password data is transmitted along with identification number data and random number data, the electronic security key is enabled to verify authenticity of electronic security key.

DESCRIPTION OF DRAWING(S) - The figure shows the flow chart illustrating communication between electronic security key and coin acceptor.

pp; 49 DwgNo 6/11

Title Terms: ELECTRONIC; SECURE; KEY; ELECTRONIC; COIN; ACCEPT; ENCRYPTION; ALGORITHM; GENERATE; ENCRYPTION; PASSWORD; DATA; TRANSMIT; ELECTRONIC; COIL; ACCEPT; ENABLE; COIN; PROGRAM
Derwent Class: T01; T05; W01; W04
International Patent Class (Main): **G06F-007/02** ; G06K-005/00; G07D-005/00; H04L-009/32

9/5/13 **(Item 13 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

012389655 **Image available**
WPI Acc No: 1999-195762/199917
Related WPI Acc No: 1998-045028; 2002-262277
XRPX Acc No: N99-144032

Computer implemented electronic information processing system e.g. for MIDI data - performs processing of data classified from main information based on predefined algorithm **which is produced** according **to additional** data **included in main information**

Patent Assignee: YAMAHA CORP (NIHG)
Inventor: TARUGUCHI H
Number of Countries: 002 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 11039796	A	19990212	JP 97193128	A	19970702	199917 B
GB 2354857	A	20010404	GB 9713555	A	19970626	200120
			GB 200023084	A	20000920	
GB 2354858	A	20010404	GB 9713555	A	19970626	200120
			GB 200023087	A	20000920	
GB 2354860	A	20010404	GB 9713555	A	19970626	200120
			GB 200023095	A	20000920	
GB 2354857	B	20010516	GB 9713555	A	19970626	200128
			GB 200023084	A	20000920	
GB 2354858	B	20010530	GB 9713555	A	19970626	200131
			GB 200023087	A	20000920	
GB 2354860	B	20010530	GB 9713555	A	19970626	200131
			GB 200023095	A	20000920	
JP 3178378	B2	20010618	JP 97193128	A	19970702	200136

Priority Applications (No Type Date): JP 97148612 A 19970522; JP 96191528 A 19960702
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11039796	A		24	G11B-020/10	
GB 2354857	A			G06F-001/00	Derived from application GB 9713555
GB 2354858	A			G06F-001/00	Derived from application GB 9713555
GB 2354860	A			G06F-001/00	Derived from application GB 9713555
GB 2354857	B			G06F-001/00	Derived from application GB 9713555
GB 2354858	B			G06F-001/00	Derived from application GB 9713555
GB 2354860	B			G06F-001/00	Derived from application GB 9713555
JP 3178378	B2		25	G10H-001/00	Previous Publ. patent JP 11039796

Abstract (Basic): JP 11039796 A

NOVELTY - A portion of data groups in main information is classified based on predetermined small data pieces of 1 bit size characteristics. The classified data are processed based on a predefined algorithm which is produced based on some additional copyright display data and recording format data included in the main information.

USE - For processing of MIDI data of electronic musical instrument using personal computer.

ADVANTAGE - Prevents unjust operation. DESCRIPTION OF DRAWING(S) - The figure shows data conversion format used during MIDI data processing.

Dwg.1/10

Title Terms: COMPUTER; IMPLEMENT; ELECTRONIC; INFORMATION; PROCESS; SYSTEM; MIDI; DATA; PERFORMANCE; PROCESS; DATA; CLASSIFY; MAIN; INFORMATION;

BASED; PREDEFINED; ALGORITHM; PRODUCE; ACCORD; ADD; DATA; MAIN; INFORMATION

Derwent Class: P85; P86; T03; W04

International Patent Class (Main): **G06F-001/00** ; G10H-001/00; G11B-020/10

International Patent Class (Additional): **G06F-012/14** ; G09C-005/00; G10K-015/02; G10L-011/00; G11B-020/00; H04N-001/32

File Segment: EPI; EngPI

9/5/14 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012320863 **Image available**
WPI Acc No: 1999-126969/199911
XRPX Acc No: N99-093149
Automatic installation system of latest version of control software for peripheral component of computer - updates memory relevant control software automatically based on **driver difference** data **and updating** algorithm **corresponding to connected peripheral equipment**
Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11003220	A	19990106	JP 97153321	A	19970611	199911	B

Priority Applications (No Type Date): JP 97153321 A 19970611
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11003220	A		6	G06F-009/06	

Abstract (Basic): JP 11003220 A
NOVELTY - The personal computer system recognises the connection of peripheral equipment (111) automatically and loads into memory relevant control software (105). This software updates itself to corresponding version using the driver difference data (113) and updating algorithm (112).
USE - For personal computer systems during peripheral equipment connection.
ADVANTAGE - Ensures use of latest version of software. DESCRIPTION OF DRAWING(S) - The figure shows block diagram of the computer system. (105) Control software; (111) Peripheral equipment; (112) Updating algorithm; (113) Driver difference data.
Dwg.1/4
Title Terms: AUTOMATIC; INSTALLATION; SYSTEM; LATE; VERSION; CONTROL; SOFTWARE; PERIPHERAL; COMPONENT; COMPUTER; UPDATE; MEMORY; RELEVANT; CONTROL; SOFTWARE; AUTOMATIC; BASED; DRIVE; DIFFER; DATA; UPDATE; ALGORITHM; CORRESPOND; CONNECT; PERIPHERAL; EQUIPMENT
Derwent Class: T01
International Patent Class (Main): **G06F-009/06**
International Patent Class (Additional): **G06F-013/10**

9/5/16 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012130010 **Image available**
WPI Acc No: 1998-546922/199847
XRPX Acc No: N98-426152
Automatic software production apparatus - develops partial program source into frame program source using developing algorithm , based on **input** data , **which is further developed into real program source**
Patent Assignee: TOKYO ELECTRIC CO LTD (TODK)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10240514	A	19980911	JP 9744115	A	19970227	199847	B

Priority Applications (No Type Date): JP 9744115 A 19970227
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10240514	A		6	G06F-009/06	

Abstract (Basic): JP 10240514 A
The apparatus has an input unit, through which data (12,13) including information regarding screen item definition and partial program source developing condition are input. A controller controls the input operation.
The partial program source is developed into a frame program source, using a developing **algorithm based on** the input **data** . Then, the developed partial program source is further developed into a real program source.
ADVANTAGE - Enables supplying partial program source corresponding to demand specification of software. Conserves memory capacity and improves usage efficiency of memory. Improves operativity, by simplifying selection of partial program source.
Dwg.2/7
Title Terms: AUTOMATIC; SOFTWARE; PRODUCE; APPARATUS; DEVELOP; PROGRAM; SOURCE; FRAME; PROGRAM; SOURCE; DEVELOP; ALGORITHM; BASED; INPUT; DATA; DEVELOP; REAL; PROGRAM; SOURCE
Derwent Class: T01
International Patent Class (Main): **G06F-009/06**
File Segment: EPI

9/5/20 (Item 20 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011656699 **Image available**
WPI Acc No: 1998-073607/199807
XRPX Acc No: N98-058978
File protective management apparatus for data processor - has master management identification holder which stores predetermined data with predetermined algorithm **that is formed** based on **time** data
Patent Assignee: FUJITSU LTD (FUIT)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9311807	A	19971202	JP 96127056	A	19960522	199807	B

Priority Applications (No Type Date): JP 96127056 A 19960522
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9311807	A		5	G06F-012/00	

Abstract (Basic): JP 9311807 A
The apparatus includes a starting unit (6) which starts master management identification generator (8). The ID generator produces a predetermined data with a predetermined **algorithm** , **based on** a time **data** . A master management ID holder (9) stores the generated ID data.
ADVANTAGE - Master management ID can be varied for short time. Prevents illegal access of time.
Dwg.1/3
Title Terms: FILE; PROTECT; MANAGEMENT; APPARATUS; DATA; PROCESSOR; MASTER; MANAGEMENT; IDENTIFY; HOLD; STORAGE; PREDETERMINED; DATA; PREDETERMINED; ALGORITHM; FORMING; BASED; TIME; DATA
Derwent Class: T01
International Patent Class (Main): **G06F-012/00**
International Patent Class (Additional): **G06F-012/14**
File Segment: EPI

9/5/24 (Item 24 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008736031 **Image available**
WPI Acc No: 1991-240047/199133
XRPX Acc No: N91-183071

Image mask generation method for image processing - has mask pixel value determined according to pre-specified algorithm based on mask creation array pixel value

Patent Assignee: CROSFIELD ELECTRONICS LTD (CROE)
Inventor: FREEMAN S

Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 441498	A	19910814	EP 91300490	A	19910123	199133	B
EP 441498	A3	19930317	EP 91300490	A	19910123	199350	

Priority Applications (No Type Date): GB 902478 A 19900205
Cited Patents: NoSR.Pub; 2.Jnl.Ref; EP 344976; GB 2140257; JP 62019970
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 441498	A				

Designated States (Regional): DE GB

Abstract (Basic): EP 441498 A

The method of generating an image mask defining a region of an image consists of the steps of for each pixel of the image, determining whether the colour of the pixel satisfies predetermined conditions. If it does, a control data creation array is positioned over the corresponding mask pixel.

For each mask pixel a mask value is generated according to a predetermined **algorithm based on** the control **data** creation array pixel values and corresponding current mask pixel values. The creation array has a set of pixels defining a three dimensional profile of data values selected from a group of at least three values.

USE/ADVANTAGE - Method is fast and capable of generating soft-edged masks. (10pp Dwg.No.1/6

Title Terms: IMAGE; MASK; GENERATE; METHOD; IMAGE; PROCESS; MASK; PIXEL; VALUE; DETERMINE; ACCORD; PRE; SPECIFIED; ALGORITHM; BASED; MASK; CREATION; ARRAY; PIXEL; VALUE
Derwent Class: T01
International Patent Class (Additional): **G06F-015/72**
File Segment: EPI

22/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015518338 **Image available**
WPI Acc No: 2003-580485/200355
XRPX Acc No: N03-461575
Data ciphering device for facsimile, updates initial value used for encipherment of data in cipher **text block chain system,** based on data **regarding date/year/month and time**
Patent Assignee: MITA IND CO LTD (MTAI)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 6339035	A	19941206	JP 93151519	A	19930528	200355	B

Priority Applications (No Type Date): JP 93151519 A 19930528
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 6339035	A		8	H04N-001/44	

Abstract (Basic): JP 6339035 A
NOVELTY - A signal obtained by encoding binarized picture data, is enciphered in a cipher text block chain (CBC) system. The cipher text is modulated by a modem (17) received through a public telephone line. The demodulated text is decoded and changed into ordinary sentence which is decoded by a decoder (16). The value used for encipherment is updated based on data regarding the date/year/month and time.
USE - Data ciphering for facsimile.
ADVANTAGE - Enables performing the enciphering easily and reliably by enciphering the encoded signal in the ciphered text block chain system.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the data ciphering device. (Drawing includes non-English language text).
decoder (16)
modem (17)
pp; 8 DwgNo 1/1
Title Terms: DATA; CIPHER; DEVICE; FACSIMILE; UPDATE; INITIAL; VALUE; DATA; CIPHER; TEXT; BLOCK; CHAIN; SYSTEM; BASED; DATA; DATE; YEAR; MONTH; TIME
Derwent Class: P85; U21; W01; W02
International Patent Class (Main): H04N-001/44
International Patent Class (Additional): G04G-015/00; G09C-001/00; **H04L-009/00** ; **H04L-009/10** ; **H04L-009/12**
File Segment: EPI; EngPI

22/5/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008505438 **Image available**
WPI Acc No: 1991-009522/199102
XRPX Acc No: N91-007445
Data ciphering and deciphering system - uses successive individual stages each using cipher **values** dependent **on received** data
Patent Assignee: ZAHN M (ZAHN-I)
Inventor: ZAHN M
Number of Countries: 002 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 406457	A	19910109	EP 89112107	A	19890703	199102	B

Priority Applications (No Type Date): EP 89112107 A 19890703
Cited Patents: DE 3244537; EP 202989
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 406457	A				

Designated States (Regional): DE FR

Abstract (Basic): EP 406457 A
The ciphering and deciphering system uses a number of successive steps (S1...Sn) with the cipher values for each individual step (S1...Sn) determined in dependence on the data to be ciphered via an electronic coding circuit (EC).
In each step (S1...Sn) only part (B) of the data is ciphered, the remainder (A) being unchanged, with the cipher values (K) provided by the cipher generator (KG) dependent only on the unchanged data (A). The number of individual steps (S1...Sn) is sufficient to ensure that all the data is ciphered at least once.
USE - For ensuring security of computer data.
Dwg.1/2
Title Terms: DATA; CIPHER; DECIPHER; SYSTEM; SUCCESSION; INDIVIDUAL; STAGE; CIPHER; VALUE; DEPEND; RECEIVE; DATA
Derwent Class: T01; W01
International Patent Class (Additional): **H04L-009/06**
File Segment: EPI

26/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06277702 **Image available**
LICENSE CARD MANUFACTURING SYSTEM

PUB. NO.: 11-219291 [JP 11219291 A]
PUBLISHED: August 10, 1999 (**19990810**)
INVENTOR(s): YAMAMOTO KAZUYUKI
APPLICANT(s): NIPPON CHEMICON CORP
APPL. NO.: 10-035484 [JP 9835484]
FILED: February 02, 1998 (19980202)
INTL CLASS: G06F-009/06; G06F-012/14; G09C-001/00; **H04L-009/10** ; **H04L-009/32**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a license card manufacturing system of for preventing decoding key data from being illegally used by a third person.

SOLUTION: In this manufacture system of the license card for writing the decoding key data from a master IC card for storing at least the decoding key data for decoding ciphered program data and duplication number-of-times data to an IC card and performing duplication, when the decoding key data are written to the IC card, the decoding key data **ciphered based on** prescribed common key **data** are outputted from the master IC card. The ciphered decoding key data are restored by the common key data and stored in the IC card and the duplication number-of-times data are subtracted every time the write is executed into the IC card.

26/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

06168307 **Image available**
CIPHER CONVERSION METHOD, CIPHER CONVERSION APPARATUS, DECODING METHOD, DECODING APPARATUS, AND DATA COMMUNICATION SYSTEM

PUB. NO.: 11-109853 [JP 11109853 A]
PUBLISHED: April 23, 1999 (**19990423**)
INVENTOR(s): AIKAWA SHIN
TAKARAGI KAZUO
KOREEDA HIROYUKI
SASAMOTO MANABU
OKAMOTO HIROO
NOGUCHI TAKAHARU
FURUYA SOICHI
HIRAHATA SHIGERU
APPLICANT(s): HITACHI LTD
APPL. NO.: 10-222636 [JP 98222636]
FILED: August 06, 1998 (19980806)
PRIORITY: 09213327 [JP 979213327], JP (Japan), August 07, 1997 (19970807)
INTL CLASS: G09C-001/00; **H04L-009/06**

ABSTRACT

PROBLEM TO BE SOLVED: To make it possible to dynamically control a circulation shift from a key without **depending** upon conversion **data** and to execute **cipher** conversion having a high degree of random characteristics with a simple constitution by determining the selection sequence of a circulation shift processing selection means based on the data for determining shift number selection sequence.

SOLUTION: Inputted plaintext C101 is separated to leftmost 32 bit L[1] and rightmost 32 bit R[1] and thereafter, the cipher conversion from a conversion section first stage 201 to conversion section 10th stage 203 is repetitively executed and finally L[11] of the leftmost 32 bits and R[11] of the rightmost 32 bits are coupled, thereby, the ciphertext M105 of 64 bits is outputted. The conversion processing in the conversion section N-th stage 202 is defined by control signals G1 to G3 outputted from a circulation shift number forming section N-th stage 205 with the 3 bit values of KG{3N-1}, KG{3N-2}, KG{3N-3} of a work key KA102, work key KB103 and work key KG104 as input. KG{x} denotes the x-bit of KG.

26/5/4 (Item 4 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2005 JPO & JAPIO. All rts. reserv.

06065728 **Image available**
CIPHER PROCESSOR, CIPHER PROCESSING METHOD AND STORAGE MEDIUM STORING CIPHER PROCESSING PROGRAM

PUB. NO.: 11-007239 [JP 11007239 A]
PUBLISHED: January 12, 1999 (**19990112**)
INVENTOR(s): OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO
MARUYAMA MASAKATSU
APPLICANT(s): MATSUSHITA ELECTRIC IND CO LTD
APPL. NO.: 10-114009 [JP 98114009]
FILED: April 23, 1998 (19980423)
PRIORITY: 09105609 [JP 979105609], JP (Japan), April 23, 1997 (19970423)
INTL CLASS: G09C-001/00; **H04L-009/06** ; **H04L-009/18**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a cipher processor improving safety without remarkably increasing a device scale and a processing time, etc.
SOLUTION: This device is a data ciphering device 10 performing cipher processing specified by the key data and generating a ciphered message from a plain text, and is provided with a block storage part 102 storing the chain data to be used for affecting the former data to the later data and updating the chain data whenever the cipher processing is performed, a key data fusion part 103 fusing the chain data stored in the block storage part 102 to the key data and generating the fusion key data and the first - eight ciphering parts 105a-h performing the **cipher** processing **based on** the fusion key **data** , generating the **ciphered** message and outputting the middle data generated in a process until the ciphered message is generated. Then, the block storage part 102 updates the chain data stored in itself with the middle data outputted from the first - eight ciphering parts 105a-h as the new chain data to make them use to the next cipher processing.

26/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

05946292 **Image available**
AUTHENTICATION SYSTEM AND AUTHENTICATION METHOD

PUB. NO.: 10-229392 [JP 10229392 A]
PUBLISHED: August 25, 1998 (**19980825**)
INVENTOR(s): HIKITA JUNICHI
IKUTO YOSHIHIRO
CHIMURA SHIGEMI
APPLICANT(s): ROHM CO LTD [365425] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-029182 [JP 9729182]
FILED: February 13, 1997 (19970213)
INTL CLASS: [6] **H04L-009/16** ; G06K-017/00; G09C-001/00; **H04L-009/32** ; H04M-015/00
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.4 (COMMUNICATION -- Telephone); 44.9 (COMMUNICATION -- Other); 45.3 (INFORMATION PROCESSING -- Input Output Units)
JAPIO KEYWORD:R073 (TRANSPORTATION -- Automatic Wickets); R303

ABSTRACT

PROBLEM TO BE SOLVED: To provide an IC card which is difficult to be used by a person pretending to be a user.

SOLUTION: **Ciphering** authentication data are generated **based on** authentication fundamental **data** , including a random number part by using a ciphering rule, when a ciphering instruction is given by a ciphering authentication data generating means 5. The ciphering rule is varied according to the frequency of a given ciphering instruction. The ciphering authentication data are transmitted by a transmitting means 7. The ciphering authentication data transmitted from a second device B are received by a receiving means 9. A prohibiting instruction output means 11 judges whether or not the ciphering authentication data transmitted from the second device B match the ciphering authentication data generated, when the same frequency of the ciphering instruction is given to the ciphering authentication data-generating means of a first device A and outputs a prohibiting instruction to prohibit the transmission of the subject data to be transmitted, when a judging result is negative.

26/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

05796628 **Image available**
CIPHERING KEY SHARING METHOD

PUB. NO.: 10-079728 [JP 10079728 A]
PUBLISHED: March 24, 1998 (**19980324**)
INVENTOR(s): BABA YOSHIMI
APPLICANT(s): CARD KOOLE SERVICE KK [000000] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-023745 [JP 9723745]
FILED: February 06, 1997 (19970206)
INTL CLASS: [6] **H04L-009/08**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems); 45.9 (INFORMATION PROCESSING -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a ciphering key sharing method in which security against various attacks is enhanced while generating a common ciphering key and simplifying the ciphering communication system on a network.

SOLUTION: Fourier transformation with weighting function and center matrix processing are operated on the identifier of each entity in a center (procedures 2-1, 2-2), randomization transformation is applied the identifier based on transitory random number data generated by an artificial operation of the entity to generate a personal key specific to each entity (procedures 2-3 - 2-5), an identifier transformation **algorithm** is generated **based on** the random number **data** and the Fourier transformation with weighting function (procedure 2-6) and the algorithm and the personal key are distributed to the entity. Each entity acts the identifier transformation algorithm and the personal key onto the identifier of a communication opposite party to generate a common key for ciphering communication with a communication opposite party.

26/5/7 (Item 7 from file: 347)
DIALOG(R)File 347:JAPIO

05654927 **Image available**
CIPHERING METHOD AND CIPHERING DEVICE

PUB. NO.: 09-269727 [JP 9269727 A]
PUBLISHED: October 14, 1997 (**19971014**)
INVENTOR(s): KAWAMURA SHINICHI
APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-077397 [JP 9677397]
FILED: March 29, 1996 (19960329)
INTL CLASS: [6] G09C-001/00; **H04L-009/06** ; **H04L-009/16**
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION -- Telegraphy)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a ciphering method and a ciphering device capable of improving a ciphering strength and a ciphering processing speed by efficiently utilizing resources of hardware and software.

SOLUTION: This ciphering device generates plural intermediate keys K1-Kn **based on** inputted key **data** 112 and generates **ciphered** data 111 by performing a stirring processing with stirring functions fs of plural (n) stages with respect to input block data 110 by using these respectively generated plural intermediate key data. At this time, a key updating part 107 updates the intermediate keys Kn, K1 to be used for agitation functions fs of the last stage and the first stage each time the ciphered data 111 having a prescribed data amount are generated.

26/5/8 (Item 8 from file: 347)
DIALOG(R)File 347:JAPIO

05585397 **Image available**
SYNCHRONIZATION STREAM CIPHERING DEVICE AND DECODER APPLIED TO THE DEVICE

PUB. NO.: 09-200197 [JP 9200197 A]
PUBLISHED: July 31, 1997 (**19970731**)
INVENTOR(s): KURODA KEIICHI
APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-003628 [JP 963628]
FILED: January 12, 1996 (19960112)
INTL CLASS: [6] **H04L-009/22** ; **H04L-009/12**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems)

ABSTRACT

PROBLEM TO BE SOLVED: To provide the ciphering device by which the possibility of invasion to security is considerably precluded.

SOLUTION: A **ciphering** device 1 calculates **ciphered** data **based on** received **data** and a 1st random number string generated from a random number source 11. Oh the other hand, a decoder 2 decodes the **ciphered** data **based on** the **ciphered data** and a 2nd random number string generated from a random number source 21 and provides an output of data. Furthermore, the decoder 2 is provided with a storage circuit 22 storing sequentially the 2nd random number string and a control circuit 25 extracting a desired random number from the storage circuit 22 to recover synchronization when the synchronization between the ciphering device 1 and the decoder 2 is deviated.

04639257 **Image available**
PRIVACY TRANSMISSION SYSTEM

PUB. NO.: 06-311157 [JP 6311157 A]
PUBLISHED: November 04, 1994 (**19941104**)
INVENTOR(s): NAKADA KENJI
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 05-099415 [JP 9399415]
FILED: April 26, 1993 (19930426)
INTL CLASS: [5] **H04L-009/00** ; **H04L-009/10** ; **H04L-009/12** ; G09C-001/10
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION PROCESSING -- Memory Units)

ABSTRACT

PURPOSE: To provide a privacy system without the leakage of secret with a simple method by ciphering next transmission or reception with a **ciphering** code generated **based on data** which are transmitted or received previous time.

CONSTITUTION: When data are transmitted from a device A to device B, the **ciphering** code **based on** transmitted **data** is formed by a **ciphering** code generating means 50. Data transmitted from the device A to the device B based on the code are ciphered by a ciphering means 60. A CRC code for data error detection is generally sufficient for the ciphering code, and the ciphering code generation means 50 shared a CRC circuit 50. The CRC code is given to the read counter 3 of transmission RAM 2 and an address where the CRC is set to be an initial value is formed by an address counter. Thus, transmission data are read from an address in the middle of transmission RAM 22, and received data are written from the middle of reception RAM 32.

26/5/13 (Item 13 from file: 347)
DIALOG(R)File 347:JAPIO

04508692 **Image available**
CIPHER COMMUNICATION METHOD AND CIPHER COMMUNICATION SYSTEM

PUB. NO.: 06-152592 [JP 6152592 A]
PUBLISHED: May 31, 1994 (**19940531**)
INVENTOR(s): SUZAKI SEIICHI
TAKARAGI KAZUO
FUNAKUBO KENICHI
NAKAMURA TERUO
APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
HITACHI SOFTWARE ENG CO LTD [472485] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-319457 [JP 92319457]
FILED: November 04, 1992 (19921104)
INTL CLASS: [5] **H04L-009/06** ; **H04L-009/14** ; G09C-001/00
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other)
JOURNAL: Section: E, Section No. 1599, Vol. 18, No. 467, Pg. 75, August 30, 1994 (19940830)

ABSTRACT

PURPOSE: To share a cipher key with plural communication parties in the multi- address communication by generating a cipher sentence key by means of a master key which is common to the system.

CONSTITUTION: A terminal 100 at the side of transmission ciphers a simple sentence 150 by a data key 151. A **cipher** sentence key 156 is generated **based on** a **data** key 151, address information 153 specifying a receiver, and master key 154 common to the system. A communication sentence consisting of the address information 153, cipher sentence key 156, and cipher sentence 152 is sent to a communication network 130. A terminal 101 at the side of reception generates the data key 151 from the address information 153 and cipher sentence key 156 included in the received communication sentence by means of the master key 154. By means of the generated data key 151, the cipher sentence 152 is decoded to generate the simple sentence 150. In short, as master key 154 is common to the system, the same data key 151 can be used between the transmitter and receiver terminals. In addition, the data key 151 is disposable and its safety is dependable.

26/5/14 (Item 14 from file: 347)
DIALOG(R)File 347:JAPIO

04324403 **Image available**
COMMUNICATION SYSTEM FOR CIPHERED CONTROL SIGNAL

PUB. NO.: 05-316103 [JP 5316103 A]
PUBLISHED: November 26, 1993 (**19931126**)
INVENTOR(s): NOGUCHI YOSHIRO
ADACHI KAZUO
APPLICANT(s): MITSUBISHI ELECTRIC CORP [000601] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-142078 [JP 92142078]
FILED: May 08, 1992 (19920508)
INTL CLASS: [5] **H04L-009/06** ; **H04L-009/14**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 1517, Vol. 18, No. 124, Pg. 67, February 28, 1994 (19940228)

ABSTRACT

PURPOSE: To devise the ciphered control signal not easily decoded by revising random number series data used for ciphering the control signal as required.

CONSTITUTION: One random number key generating section is selected from plural random number key generating sections 2c, 2d generating prescribed random number data, and a control signal is ciphered at a control signal **ciphering** circuit 2f **based on** random number **data** generated by the selected random number key generating section. Moreover, random number key identification data representing the random number key generating section used for the ciphering are added to the ciphered control signal. Then the ciphered control signal with the random number key identification data added thereto is sent/received between a master station 2 and a slave station 8 to implement the communication, a control signal decoder 9 extracts the original control signal based on the random number key identification data from the ciphered control signal and decodes it. Thus, the ciphered control signal is not easily decoded.

26/5/16 (Item 16 from file: 347)
DIALOG(R)File 347:JAPIO

04276788 **Image available**
CIPHERING TRANSMISSION RECEPTION METHOD IN RADIO LINE AND EQUIPMENT USING THE METHOD

PUB. NO.: 05-268488 [JP 5268488 A]
PUBLISHED: October 15, 1993 (**19931015**)
INVENTOR(s): TSUKUI NAOHIKO
APPLICANT(s): JAPAN RADIO CO LTD [000433] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-064890 [JP 9264890]
FILED: March 23, 1992 (19920323)
INTL CLASS: [5] H04N-001/44; G06F-015/66; G09C-001/00; **H04L-009/34**
JAPIO CLASS: 44.7 (COMMUNICATION -- Facsimile); 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other); 45.4 (INFORMATION PROCESSING -- Computer Applications)
JOURNAL: Section: E, Section No. 1496, Vol. 18, No. 47, Pg. 10, January 25, 1994 (19940125)

ABSTRACT

PURPOSE: To obtain the ciphering transmission reception method with high **ciphering** performance **based on** abundant **data** quantity and the equipment using the method in which quick transmission is implemented.

CONSTITUTION: A sender side adds a series and a code generated based on the series to a synchronizing phase signal area 201 to block a picture data signal area into blocks 202. Moreover, codes are arranged through synchronization to obtain a synchronizing signal and a picture data signal is sent continuously while starting from an optional position in the unit of blocks 202 based on the synchronizing signal. A receiver side receives the synchronizing signal and the picture data signal and demodulates them and stores demodulation data of the picture data signal. Furthermore, the series of the code is detected from the synchronizing signal and the series is compared with the stored same series as that of the sender side in the unit of prescribed lines to detect a line number of the demodulation data, prescribed number of lines are replaced based on the ciphering code and a normal picture is obtained from the demodulation data

26/5/19 (Item 19 from file: 347)
DIALOG(R)File 347:JAPIO

03116627 **Image available**
ENCIPHERING SYSTEM

PUB. NO.: 02-092127 [JP 2092127 A]
PUBLISHED: March 30, 1990 (**19900330**)
INVENTOR(s): NAKAMURA KENGO
APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 63-242596 [JP 88242596]
FILED: September 29, 1988 (19880929)
INTL CLASS: [5] **H04L-009/06** ; **H04L-009/14** ; **H04L-009/32**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 943, Vol. 14, No. 288, Pg. 124, June 21, 1990 (19900621)

ABSTRACT

PURPOSE: To prevent the leakage of data by using data before transmission with a first system, using data after decoding with a second system, preparing a new encipherment table with a password generating part having the same algorithm, rewriting the encipherment table of both system and using it as the encipherment table of the next data transmission.

CONSTITUTION: A transmission side system A enciphers the transmission data with an encipherment table 1, forms encipherment data for transmission, transmits them, forms the data to update the encipherment table 1 with a special **algorithm** (computation expression) **based on** the transmission **data** and the data of the encipherment table 1 and thus, the encipherment table is updated. A reception side system B has an encipherment table 2 of the same sequence as that of a transmission side, decodes the received encipherment sentence based on the encipherment number table, forms the new encipherment table by the same algorithm as that of a transmission side based on the decoded data and the encipherment table 2 and updates the encipherment table. Thus, the leakage of the transmission data can be prevented.

NPL
Bib

```
Set     Items   Description
S1      15360   CIPHER? OR CYPHER?
S2    2184858   ALGORITHM? ?
S3    7577280   DATA
S4     159898   (BASED()ON OR ACCORDING? OR CONTINGENT? OR
           EPENDING)(3W)S3
S5       2484   (S1 OR S2)(5N) S4
S6         18   S1 (5N) S4
S7          2   S6 NOT PY>1999
S8       1911   S2 (3N) S4
S9      45447   ((BREAK? OR BROKEN)()APART OR SEPARATE? ? OR SEPARATING OR
           SEPERATION OR PARTITION? OR FRAGMENT? OR SEGMENT? OR DIVIDE? ?
            OR DIVIDING)(3N)(S1 OR S2)
S10        37   S9 (3N) S4
S11        49   S9 (5N) S4
S12        20   S11 NOT PY>1999
S13        14   RD  (unique items)
File   8:Ei Compendex(R) 1970-2005/Dec W2
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Nov
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Dec W3
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1898-2005/Dec W2
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Oct W3
         (c)2005 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Dec 20
         (c) 2005 The Gale Group
File   6:NTIS 1964-2005/Dec W2
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Dec W2
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Dec W2
         (c) 2005 Inst for Sci Info
File  62:SPIN(R) 1975-2005/Oct W2
         (c) 2005 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Oct
         (c) 2005 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2005/Nov W2
         (c) 2005 FIZ TECHNIK
File  56:Computer and Information Systems Abstracts 1966-2005/Dec
         (c) 2005 CSA.
File  57:Electronics & Communications Abstracts 1966-2005/Dec
         (c) 2005 CSA.
```

13/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04373554 E.I. No: EIP96013006849
Title: Informatique et amelioration des performances dans les entrepots modernes
Title: Information technology and improving performances in modern warehouses
Author: Fleury, Gilles
Corporate Source: INFFLUX (Informatique et Flux)
Source: REE, Revue de L'Electricite et de L'Electronique n 6 Dec 1995. p 41-46
Publication Year: 1995
CODEN: REELF3 ISSN: 1265-6534
Language: French
Document Type: JA; (Journal Article) Treatment: A; (Applications); G; (General Review)
Journal Announcement: 9605W5
Abstract: By examining the management of physical flows within companies software may be created to facilitate warehouse management. More especially, management which takes into account the 'flurry' concept - a set of orders prepared simultaneously - optimizes preparatory circuits and fork-lift movements, and keeps parcels and orders **separate** . A packing **algorithm** , with calculations **based on** order **data** regarding the number, size and contents of parcels, constitutes another important aspect of the physical flow management system. Installing an optimized logistical system requires a large initial investment, but will bring numerous advantages. (Author abstract)
Descriptors: *Industrial management; Computer software; Materials handling; Warehouses; Optimization; Packaging; Algorithms; Calculations
Identifiers: Warehouse management; Fork lift movements; Physical flow management system
Classification Codes:
912.2 (Management); 723.1 (Computer Programming); 694.4 (Storage); 921.5 (Optimization Techniques); 694.1 (Packaging)
912 (Industrial Engineering & Management); 723 (Computer Software); 691 (Bulk Materials Handling); 694 (Packaging & Storing); 921 (Applied Mathematics)
91 (ENGINEERING MANAGEMENT); 72 (COMPUTERS & DATA PROCESSING); 69 (MATERIALS HANDLING); 92 (ENGINEERING MATHEMATICS)

13/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02777775 E.I. Monthly No: EI8908074155
Title: Segmentation and object extraction algorithm with linear memory and time constraints.
Author: Anbalagan, R. S.; Hu, G.; Jain, A. K.
Corporate Source: Innovision Corp, Madison, WI, USA
Conference Title: 9th International Conference on Pattern Recognition
Conference Location: Rome, Italy Conference Date: 19881114
Sponsor: Int Assoc for Pattern Recognition, Paris, Fr
E.I. Conference No.: 12072
Source: Proceedings - International Conference on Pattern Recognition 9th.. Publ by IEEE, New York, NY, USA. Available from IEEE Service Cent (cat n 88CH2614-6), Piscataway, NJ, USA. p 596-600
Publication Year: 1988
CODEN: PICREG ISBN: 0-8186-0878-1
Language: English
Document Type: PA; (Conference Paper) Treatment: X; (Experimental); A; (Applications)
Journal Announcement: 8908
Abstract: An experimental segmentation and object extraction algorithm is described. The system was developed for medical image processing with the primary application being DNA (deoxyribonucleic acid) sequencing. A typical DNA sequencing can involve processing the image of an autodiagram of size 14 multiplied by 17 inches resulting in a 2048 multiplied by 8600 digitized image under the specified spatial resolutions. The digitized image is too big to manage, even using super-minicomputers such as DEC VAX 11/780, and to perform any amount of classical image processing. Therefore, an elegant hardware and software design is necessary to deal with the large image and to complete the image-understanding task in an efficient manner. This work focuses on the image-processing aspects of the system and describes the run-length image representation, a link list data structure, a heuristic connected component analysis algorithm **based on** the **data** structure, a primitive object **segmentation algorithm** , and feature extraction. 8 Refs.
Descriptors: *IMAGE PROCESSING--*Medical Applications; PATTERN RECOGNITION; ARTIFICIAL INTELLIGENCE; BIOCHEMISTRY--DNA Sequences; DATA PROCESSING--Data Structures; SYSTEMS SCIENCE AND CYBERNETICS--Heuristic Programming
Identifiers: OBJECT EXTRACTION ALGORITHM; DNA SEQUENCING; KNOWLEDGE BASED IMAGE SEGMENTATION
Classification Codes:
723 (Computer Software); 461 (Biotechnology)
72 (COMPUTERS & DATA PROCESSING); 46 (BIOENGINEERING)

13/5/6 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

06842355 INSPEC Abstract Number: C9804-6160S-012
Title: Parallel algorithms for spatial data partition and join processing
Author(s): Yanchun Zhang; Jitian Xiao; Roberts, A.J.
Author Affiliation: Dept. of Maths & Comput., Univ. of Southern Queensland, Toowoomba, Qld., Australia
Conference Title: 1997 3rd International Conference on Algorithms and Architectures for Parallel Processing. ICA/sup 3/PP 97 (IEEE Cat. No.97TH8324) p.703-16
Editor(s): Goscinski, A.; Hobbs, M.; Zhou, W.
Publisher: World Scientific, Singapore
Publication Date: 1997 Country of Publication: Singapore xiii+765 pp.
ISBN: 0 7803 4229 1 Material Identity Number: XX97-02966
U.S. Copyright Clearance Center Code: 0 7803 4229 1/97/$10.00
Conference Title: Proceedings of 3rd International Conference on Algorithms and Architectures for Parallel Processing
Conference Sponsor: Deakin Univ; IEEE Victorian Sect
Conference Date: 10-12 Dec. 1997 Conference Location: Melbourne, Vic., Australia
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Theoretical (T)
Abstract: The spatial join operations combine two sets of spatial data by their spatial relationships. They are among the most important, yet most time-consuming operations in spatial databases. We consider the problem of binary polygon intersection joins based on the filter-and-refine strategy. Our objective is to minimize the I/O cost and the response time for the refinement step. First, a graph model is proposed to formalize the refinement cost and matrix-based sequential data partition algorithms are introduced. Then a parallel data partitioning algorithm is developed with a detailed complexity analysis. **Based on** the **data partition** results, a distribution **algorithm** is also proposed for scheduling parallel spatial join processing. (10 Refs)
Subfile: C
Descriptors: computational complexity; database theory; parallel algorithms; query processing; relational algebra; relational databases; scheduling; spatial data structures; visual databases
Identifiers: parallel algorithms; spatial data partition; join processing ; spatial join operations; spatial databases; binary polygon intersection joins; filter-and-refine strategy; input output cost; response time; graph model; refinement cost; matrix-based sequential data partition; parallel data partitioning algorithm; complexity analysis; scheduling
Class Codes: C6160S (Spatial and pictorial databases); C6120 (File organisation); C6150N (Distributed systems software); C4250 (Database theory); C6160D (Relational databases)

13/5/10 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

01365838 INSPEC Abstract Number: C72008294
Title: Algorithm of circuit decomposition when designing digital computers with self-diagnosis
Author(s): Babushkina, N.A.; Vedeshenkov, V.A.; Vlasenko, N.A.; Volkov, A.F.
Conference Title: Proceedings of the 5th all-union conference on control problems Part III p.97-100
Publisher: Nat. Committee of Automatic Control of the USSR, Moscow, USSR
Publication Date: 1971 Country of Publication: USSR 200 pp.
Conference Sponsor: Nat. Committee of Automatic Control of the USSR
Conference Date: 4-8 Oct. 1971 Conference Location: Moscow, USSR
Language: Russian Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: The problem concerns the minimization of control points when dividing a given circuit into **separate** sub-circuits. The **algorithm** is additionally **based on data** giving the upper limit of costs for providing the control points and the characteristics of an oriented graph which is equivalent to the considered circuit. (1 Refs)
Subfile: C
Descriptors: computer architecture; graph theory; minimisation
Identifiers: self diagnosis; circuit decomposition; digital computers; minimization; control points; upper limit; costs; oriented graph
Class Codes: C5220 (Computer architecture)

13/5/14 (Item 2 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

00995733 Genuine Article#: FL808 Number of References: 19
Title: ALGORITHM TO PREDICT TRIPLE-VESSEL LEFT MAIN CORONARY-ARTERY DISEASE IN PATIENTS WITHOUT MYOCARDIAL-INFARCTION - AN INTERNATIONAL CROSS VALIDATION
Author(s): DETRANO R; JANOSI A; STEINBRUNN W; PFISTERER M; SCHMID JJ; MEYER MM; GUPPY KH; ABIMANSOUR P
Corporate Source: HARBOR UNIV CALIF LOS ANGELES,CTR MED,ST JOHNS CARDIAC RES CTR,1124 W CARSON ST,BLDG A-17/TORRANCE//CA/90502; VET ADM MED CTR,DEPT MED,DIV CARDIOL/LONG BEACH//CA/90822
Journal: CIRCULATION, 1991, V83, N5, P89-96
Language: ENGLISH Document Type: ARTICLE
Geographic Location: USA
Subfile: SciSearch; CC LIFE--Current Contents, Life Sciences; CC CLIN--Current Contents, Clinical Medicine
Journal Subject Category: CARDIOVASCULAR SYSTEM; HEMATOLOGY
Abstract: Logistic regression was applied to the clinical, risk factor, and exercise data of consecutive angiographic referrals without prior myocardial infarction to determine an algorithm predicting the probability of triple-vessel/left main coronary artery disease. These data were obtained from a total of 1,074 such subjects from patient populations at four centers (Cleveland Clinic Foundation, Cleveland, Ohio; Hungarian Institute of Cardiology, Budapest, Hungary; the university hospitals, Zurich and Basel, Switzerland; and the Veterans Administration Medical Center, Long Beach, Calif.) and used to derive four **separate** probability **algorithms** . Each **algorithm** is **based on** patient **data** from study samples at three of the four centers and consists of 272 logistic functions, which are related to linear combinations of 13 variables (age, sex, type of chest pain, systolic blood pressure, resting electrocardiogram, serum cholesterol, fasting blood sugar, achieved exercise work load, achieved heart rate, exercise-induced angina and hypotension, heart rate-adjusted resting ST depression, and exercise ST slope). The four algorithms were cross validated by testing them on the populations not involved in their derivation. The resulting probabilities in the four test groups were then compared with the angiographic findings of triple-vessel/left main coronary artery disease. The discriminatory power of all the algorithms was fair to good (area under receiver operating characteristic curve, 0.68, 0.75, 0.82, 0.85) in the test groups. The algorithm did not significantly underestimate or overestimate disease probability except in one center (Long Beach). The findings suggest that a clinician could expect to avert at least 10 angiograms on patients with less severe disease for every missed case of triple-vessel/left main coronary artery disease by using these probabilities as a basis for the decision to perform angiography.
Descriptors--Author Keywords: PROBABILITY ANALYSIS; DISEASE PREDICTION; CORONARY ARTERY DISEASE
Identifiers--KeyWords Plus: DIAGNOSIS; SURGERY; PROBABILITY; SURVIVAL
Research Fronts: 89-0758 001 (MYOCARDIAL REPERFUSION INJURY; INFARCT SIZE; CONTRACTILE FUNCTION)
89-1183 001 (QUANTITATIVE CORONARY ANGIOGRAPHY; REGIONAL MYOCARDIAL PERFUSION; DISTAL FLOW RESERVE)
89-3469 001 (DIGITAL RADIOGRAPHY; RECEIVER OPERATING CHARACTERISTIC ANALYSIS; CONVENTIONAL CHEST IMAGING; DETECTION OF SIMULATED PULMONARY NODULES)
Cited References:
CIRCULATION S2, 1982, V65, P67
BRAUNWALD E, 1983, V309, P1181, NEW ENGL J MED
CAMPBELL RW, 1985, V88, P287, CHEST
DETRANO R, 1989, V64, P304, AM J CARDIOL
DETRANO R, 1984, V69, P531, CIRCULATION

DETRANO R, 1986, V8, P836, J AM COLL CARDIOL
DETRE K, 1977, V40, P212, AM J CARDIOL
DETRY JMR, 1985, V6, P227, EUR HEART J
DIAMOND GA, 1979, V300, P1350, NEW ENGL J MED
ELLIS S, 1988, V11, P908, J AM COLL CARDIOL
HANLEY JA, 1983, V148, P839, RADIOLOGY
HILDEN J, 1978, V17, P227, METHOD INFORM MED
HLATKY MA, 1988, V11, P237, J AM COLL CARDIOL
MELIN JA, 1983, V4, P622, EUR HEART J
PHILBRICK JT, 1980, V46, P807, AM J CARDIOL
PROUDFIT WL, 1988, V59, P641, BRIT HEART J
SANTIAGA JT, 1982, V15, P61, J ELECTROCARDIOL
SWETS JA, 1988, V240, P1285, SCIENCE
WHITE CW, 1984, V310, P819, NEW ENGL J MED